

1000-2007/001011

BUNDESREPUBLIK DEUTSCHLAND



DE 04 / 1317

REC'D 12 AUG 2004	
WIPO	PCT

BEST AVAILABLE COPY

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 28 239.4

Anmeldetag: 24. Juni 2003

Anmelder/Inhaber: ROBERT BOSCH GMBH, 70469 Stuttgart/DE

Bezeichnung: Sicherheits- und Zuverlässigkeitsbetrachtungen für Software-Hardware-Überwachungskonzepte elektronischer Steuergeräte mit Zuverlässigkeitsblockdiagrammen

IPC: G 06 F 11/00

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 23. Juli 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Strömmer

20.06.03 Sy

ROBERT BOSCH GMBH, 70442 Stuttgart

Sicherheits- und Zuverlässigkeitsbetrachtungen für Software-Hardware-Überwachungskonzepte elektronischer Steuergeräte mit Zuverlässigkeitsblockdiagrammen

Stand der Technik

Zuverlässigkeits- und Sicherheitsanforderungen an Fahrzeugfunktionen ergeben sich aus den Kundenwünschen unter Berücksichtigung der technischen, gesetzlichen und finanziellen Randbedingungen. Zuverlässigkeitsanforderungen an Fahrzeugfunktionen werden beispielsweise in Form von kurzen Reparaturzeiten oder langen Serviceintervallen vorgegeben. Sicherheitsanforderungen legen dagegen das sichere Verhalten des Fahrzeugs im Falle von Ausfällen und Störungen von Komponenten des Fahrzeugs fest. Die an Fahrzeugfunktionen gestellten Zuverlässigkeits- und Sicherheitsanforderungen legen von Anfang an auch Anforderungen an die technische Realisierung und Nachweispflichten fest. Eine der mächtigsten Maßnahmen zur Erhöhung der Sicherheit und Zuverlässigkeit ist Redundanz. Da zunehmend Fahrzeugfunktionen oder Teile von Fahrzeugfunktionen durch Software realisiert werden, haben systematische Methoden zur Zuverlässigkeits- und Sicherheitsanalyse auch zunehmenden Einfluss auf die Software-Entwicklung für elektronische Steuergeräte, etwa auf die Realisierung der Überwachungs-, Diagnose- und Sicherheitskonzepte.

Für komplexe elektronische Systeme müssen die Aktivitäten zur Absicherung der Zuverlässigkeit und Sicherheit frühzeitig geplant und in den gesamten Projektplan integriert werden.

Beschreibung der Erfindung und Vorteile

Zuverlässigkeits- und Sicherheitsanalysen umfassen z. B. Ausfallraten- und Ausfallartenanalysen, wie die Ausfallarten- und Wirkungsanalyse (FMEA) oder die Fehlerbaumanalyse (FTA), sowie die Untersuchung und Bewertung von konkreten Möglichkeiten zur Verbesserung der Zuverlässigkeit oder der Sicherheit.

Im folgenden wird am Beispiel der formalen Überprüfung von Überwachungskonzepten ein Verfahren zur formalen Überprüfung von Funktionen elektronischer Systeme durch Zuverlässigkeitsblockdiagramme beschrieben. Damit ist die frühzeitige Bewertung unterschiedlicher Überwachungskonzepte elektronischer Steuergeräte im besonderen und von Funktionen elektronischer Systeme im allgemeinen, die durch Software und Hardware realisiert werden, hinsichtlich der erreichbaren Systemsicherheit und der Systemzuverlässigkeit möglich. Die Ergebnisse beeinflussen insbesondere die Verteilung von Software-Funktionen auf die Mikrocontroller vernetzter Steuergeräte und damit die Entwicklung von Software für verteilte und vernetzte Steuergeräte.

1.1 Ausfallratenanalyse und Berechnung der Zuverlässigkeitsfunktion für Systeme

Die systematische Untersuchung der Ausfallrate einer Betrachtungseinheit ermöglicht die Voraussage der Zuverlässigkeit für die Betrachtungseinheit durch Berechnung. Diese Voraussage ist wichtig, um Schwachstellen frühzeitig zu erkennen, Alternativlösungen zu bewerten und Zusammenhänge zwischen Zuverlässigkeit, Sicherheit und Verfügbarkeit quantitativ erfassen zu können. Außerdem sind Untersuchungen dieser Art notwendig, um Zuverlässigkeitsanforderungen etwa an Komponenten stellen zu können.

Infolge von Vernachlässigungen und Vereinfachungen, sowie der Unsicherheit der verwendeten Eingangsdaten kann die berechnete, vorausgesagte Zuverlässigkeit nur ein Schätzwert für die wahre Zuverlässigkeit sein, die nur mit Zuverlässigkeitsprüfungen und Feldbeobachtungen zu ermitteln ist. Im Rahmen von Vergleichsuntersuchungen in der Analysephase spielt jedoch die absolute Genauigkeit keine Rolle, so dass besonders bei der Bewertung von Realisierungsalternativen die Berechnung der vorausgesagten Zuverlässigkeit nützlich ist.

In den folgenden Abschnitten ist die Betrachtungseinheit immer ein technisches System oder eine Systemkomponente des Fahrzeugs. Im allgemeinen Fall kann die Betrachtungseinheit auch weiter gefasst werden und beispielsweise auch den Fahrer des Fahrzeugs mit einschließen. Die Ausfallratenanalyse unterscheidet die folgenden Schritte [1]:

- Definition der Grenzen und Komponenten des technischen Systems, der geforderten Funktionen und des Anforderungsprofils
- Aufstellen des Zuverlässigkeitsblockdiagramms (engl. Reliability Block Diagram)
- Bestimmung der Belastungsbedingungen für jede Komponente
- Bestimmung von Zuverlässigkeitsfunktion oder Ausfallrate für jede Komponente
- Berechnung der Zuverlässigkeitsfunktion für das System
- Behebung der Schwachstellen

Die Ausfallratenanalyse ist ein mehrstufiges Verfahren und wird „top down“ von der Systemebene über die verschiedenen Subsystemebenen bis zur Komponentenebene der technischen Systemarchitektur durchgeführt. Die Ausfallratenanalyse muss nach Änderungen der technischen Systemarchitektur wiederholt werden.

1.1.1 Definition der Systemgrenzen, der geforderten Funktionen und des Anforderungsprofils

Für die theoretischen Überlegungen, die zur Voraussage der Zuverlässigkeit notwendig sind, müssen eingehende Kenntnisse des Systems und seiner Funktionen, sowie der konkreten Möglichkeiten zur Verbesserung der Zuverlässigkeit und Sicherheit vorausgesetzt werden.

Zum Systemverständnis zählt die Kenntnis der Architektur des Systems und seiner Wirkungsweise, die Arbeits- und Belastungsbedingungen für alle Systemkomponenten, sowie die gegenseitigen Wechselwirkungen zwischen den Komponenten, etwa in Form von Signalflüssen und der Eingangs- und Ausgangssicht aller Komponenten.

Zu den Verbesserungsmöglichkeiten gehören die Begrenzung oder die Verringerung der Belastung der Komponenten im Betrieb, etwa der statischen oder dynamischen Belastungen, der Belastung der Schnittstellen, der Einsatz besser geeigneter Komponenten, die Vereinfachung des System- oder Komponentenentwurfs, die Vorbehandlung kritischer Komponenten, sowie der Einsatz von Redundanz.

Die geforderte Funktion spezifiziert die Aufgabe des Systems. Die Festlegung der Systemgrenzen und der geforderten Funktionen bildet den Ausgangspunkt jeder Zuverlässigkeits- und Sicherheitsanalyse, weil damit auch der Ausfall definiert wird.

Zusätzlich müssen die Umweltbedingungen für alle Komponenten des Systems definiert werden, da dadurch die Zuverlässigkeit der Komponenten beeinflusst wird. So hat z. B. der

Temperaturbereich großen Einfluss auf die Ausfallrate von Hardware-Komponenten. Im Fahrzeug gehören z. B. der geforderte Temperaturbereich, der Einsatz unter Feuchtigkeit, Staub oder korrosiver Atmosphäre, oder Belastungen durch Vibrationen, Schocks oder Schwankungen, wie etwa der Versorgungsspannung zu den Umweltbedingungen. Hängen die geforderten Funktionen und die Umweltbedingungen außerdem von der Zeit ab, muss ein Anforderungsprofil festgelegt werden. Ein Beispiel für gesetzlich vorgeschriebene Anforderungsprofile im Fahrzeug sind die Fahrzyklen zum Nachweis der Einhaltung der Abgasvorschriften. In diesem Fall spricht man auch von repräsentativen Anforderungsprofilen.

1.1.2 Aufstellen des Zuverlässigkeitsblockdiagramms

Das Zuverlässigkeitsblockdiagramm gibt Antwort auf die Fragen, welche Komponenten eines Systems zur Erfüllung der geforderten Funktion grundsätzlich funktionieren müssen und welche Komponenten im Falle ihres Ausfalls die Funktion nicht grundsätzlich beeinträchtigen, da sie redundant vorhanden sind. Die Aufstellung des Zuverlässigkeitsblockdiagramms erfolgt, indem man die Komponenten der technischen Systemarchitektur betrachtet. Diese Komponenten werden in einem Blockdiagramm so verbunden, dass die zur Funktionserfüllung notwendigen Komponenten in Reihe geschaltet werden und redundante Komponenten in einer Parallelschaltung verbunden werden.

Beispiel: Aufstellen des Zuverlässigkeitsblockdiagramms für ein fiktives Brake-By-Wire-System

Für ein fiktives Brake-By-Wire-System, wie in Bild 1 dargestellt, wird zunächst die Systemgrenze festgelegt. Das System besteht aus den Komponenten Bremspedaleinheit (K_1), Steuergerät (K_2), den Radbremseinheiten (K_5, K_7, K_9, K_{11}) und den elektrischen Verbindungen ($K_3, K_4, K_6, K_8, K_{10}$).

Bei Brake-By-Wire-Systemen besteht zwischen dem Bremspedal und den Radbremsen keine hydraulische, sondern eine elektrische Verbindung. Beim Bremsen wird der Fahrerbefehl, der durch die Bremspedaleinheit K_1 vorgegeben und im Steuergerät K_2 verarbeitet wird, und die zum Bremsen notwendige Energie „by wire“ zu den Radbremseinheiten K_5, K_7, K_9 und K_{11} übertragen. Dabei muss sichergestellt werden, dass die Übernahme der Funktionen „Informations- und Energieübertragung“ zwischen Pedaleinheit und Radbremseinheiten, die bei konventionellen Bremssystemen mechanisch-hydraulisch realisiert sind, durch die elektrischen und elektronischen Komponenten K_2, K_3, K_4, K_6, K_8 und K_{10} kein zusätzliches Sicherheitsrisiko,

sondern einen Sicherheitsgewinn bringt. Die vorhersagbare Übertragung der Bremsbefehle ist deshalb eine zwingende Voraussetzung. Ebenso muss die Sicherheit auch bei Störungen und Ausfällen von Komponenten gewährleistet sein.

5 Es soll die Funktion „Bremsen“ betrachtet werden. Dafür soll die Gesamtzuverlässigkeit des Systems bestimmt werden. Es wird angenommen, dass die Ausfallraten λ_1 bis λ_{11} der Komponenten K_1 bis K_{11} bekannt sind.

10 Dieses Beispiel wird im weiteren sehr stark vereinfacht. Es soll nur die prinzipielle Vorgehensweise bei der Zuverlässigkeitsanalyse verdeutlichen. Deshalb wird nur die Informationsübertragung betrachtet, während die Aspekte der Energieversorgung und der Energieübertragung, sowie fahrdynamische Randbedingungen, wie die geforderte Bremskraftverteilung auf Vorder- und Hinterachse, die selbstverständlich auch bei der Zuverlässigkeitsanalyse berücksichtigt werden müssen, vernachlässigt werden.

15 **Bild 1:** Systemsicht für ein Brake-By-Wire-System

Für die Erfüllung der Funktion „Bremsen“ sind bei dieser vereinfachten Sicht das Funktionieren der Komponenten Bremspedaleinheit K_1 , Steuergerät K_2 , sowie der Verbindungen zwischen Bremspedaleinheit und Steuergerät K_3 zwingend notwendig.

20 Bei den Radbremseinheiten und den Verbindungen zwischen Steuergerät und Radbremseinheiten ist Redundanz vorhanden. Unter der stark vereinfachten Annahme, dass eine ausreichende Hilfsbremswirkung für das Fahrzeug mit nur einer Radbremseinheit erzielt werden kann, sind dann beispielsweise die Komponenten K_4 und K_5 notwendig, während die Komponenten K_6 und K_7 , K_8 und K_9 bzw. K_{10} und K_{11} redundant vorhanden sind. Eine derartige Anordnung wird auch als 1-aus-4-Redundanz bezeichnet.

25 Das Zuverlässigkeitsblockdiagramm für die Funktion „Bremsen“ sieht dann wie in Bild 2 dargestellt aus.

30 **Bild 2:** Zuverlässigkeitsblockdiagramm für die Funktion „Bremsen“ des Brake-By-Wire-Systems

1.1.3 Berechnung der Zuverlässigkeitsfunktion für das System

Nach Festlegung der Belastungsbedingungen und der Bestimmung der Zuverlässigkeitsfunktionen $R_i(t)$ für alle Komponenten K_i , kann unter Berücksichtigung der in Bild 3 dargestellten Grundregeln für Zuverlässigkeitsblockdiagramme [1] die Zuverlässigkeitsfunktion des Systems $R_S(t)$ berechnet werden.

Bild 3: Einige Grundregeln zur Berechnung der Zuverlässigkeitsfunktion für das System [1]

Für das Beispiel in Bild 2 kann damit die Zuverlässigkeitsfunktion des Systems R_S berechnet werden. Mit den Annahmen $R_4 = R_6 = R_8 = R_{10}$ und $R_5 = R_7 = R_9 = R_{11}$ folgt für R_S :

$$R_S = R_1 R_2 R_3 [1 - (1 - R_4 R_5)^4]$$

Wie dieses vereinfachte Beispiel zeigt, erhöht sich die Systemzuverlässigkeit für eine Funktion durch redundante Komponenten im Zuverlässigkeitsblockdiagramm gegenüber der Komponentenzuverlässigkeit. Dagegen verringert sich bei den seriell dargestellten Komponenten die Systemzuverlässigkeit gegenüber der Komponentenzuverlässigkeit. Man wird daher für die seriellen Komponenten im Zuverlässigkeitsblockdiagramm bereits eine hohe Zuverlässigkeit von den Komponenten fordern müssen oder eine technische Systemarchitektur einführen, die auch hier redundante Strukturen vorsieht.

1.2 Sicherheits- und Zuverlässigkeitsanalyse für das System mit Zuverlässigkeitsblockdiagrammen

Für die Sicherheit eines Systems ist es dagegen unwichtig, ob die Betrachtungseinheit die Funktionen erfüllt oder nicht, sofern damit kein nicht vertretbar hohes Risiko eintritt. Maßnahmen zur Erhöhung der Sicherheit werden als Schutzmaßnahmen bezeichnet und zielen auf die Verringerung des Risikos. Zuverlässigkeits- und Sicherheitsanalyse sind iterative und zusammenhängende Prozesse mit mehreren Schritten, wie in Bild 4 dargestellt.

Bild 4: Schritte bei der Zuverlässigkeits- und Sicherheitsanalyse und der Spezifikation zuverlässiger und sicherer Systeme.

5 Sie haben Einfluss auf Anforderungen an die Hardware, Software und den Software-Entwicklungsprozess für elektronische Systeme. Auch für die Sicherheitsanalyse eines Systems werden häufig Methoden zur Ausfallartenanalyse, wie FMEA oder FTA, eingesetzt. Die Ausfallartenanalyse liefert eine Bewertung des Risikos für alle Funktionen des Systems. Das zulässige Grenzkrisiko wird in der Regel durch sicherheitstechnische Festlegungen, wie
10 Gesetze, Normen oder Verordnungen, implizit vorgegeben. Aus dem ermittelten Risiko für die Funktionen des Systems und dem zulässigen Grenzkrisiko werden dann – beispielsweise anhand von Normen wie der IEC 61508 – sicherheitstechnische Anforderungen an das System abgeleitet, die oft großen Einfluss auf den System-, den Hardware- und Software-Entwurf in der Elektronikentwicklung haben.

15 Für die durch die Ausfallartenanalyse bestimmten und abgegrenzten, so genannten sicherheitsrelevanten Funktionen des Systems müssen besondere Schutzmaßnahmen getroffen werden, die beispielsweise in Hardware und Software realisiert werden können.

20 Der Nachweis der Sicherheit und Zuverlässigkeit dieser Überwachungskonzepte ist Voraussetzung für die Zulassung von Fahrzeugen zum Straßenverkehr. Im folgenden wird am Beispiel des Überwachungskonzeptes für ein E-Gas-System das Verfahren zur Beurteilung der Zuverlässigkeit und Sicherheit des Überwachungskonzeptes unter Einsatz von Zuverlässigkeitsblockdiagrammen dargestellt.

25 **Beispiel: Überwachungskonzept für ein E-Gas-System**

Als mögliche Gefahr für ein E-Gas-System wird ungewolltes Gasgeben und ein daraus folgender Unfall angenommen. Für das Motorsteuergerät bedeutet dies, dass alle diejenigen Steuerungs- und Regelungsfunktionen f_n sicherheitsrelevant sind, die zu einer unbeabsichtigten
30 Erhöhung des Motordrehmoments führen können. Für diese Funktionen ist deshalb ein Überwachungskonzept notwendig.

In diesem Beispiel soll das etwas vereinfachte Überwachungskonzept, wie es seit Jahren in Motorsteuergeräten eingesetzt wird, bezüglich der Sicherheit und Zuverlässigkeit untersucht

werden. Im Rahmen des Arbeitskreises „E-Gas“ des Verbandes der Automobilindustrie (VDA) wird dieses von der Robert Bosch GmbH entwickelte Basiskonzept derzeit zu einem standardisierten Überwachungskonzept für Motorsteuerungen von Otto- und Dieselmotoren weiterentwickelt.

5

In Bild 5 ist das Überwachungskonzept für sicherheitsrelevante Steuerungs- und Regelungsfunktionen f_n dargestellt.

Bild 5: Überwachungskonzept für sicherheitsrelevante Funktionen des Motorsteuergeräts [79]

Die sicherheitsrelevanten Steuerungs- und Regelungsfunktionen f_n werden durch die Überwachungsfunktionen f_{0n} ständig überwacht. Die Überwachungsfunktionen f_{0n} verwenden die gleichen Eingangsgrößen wie die Steuerungs- und Regelungsfunktionen f_n , arbeiten aber mit unterschiedlichen Daten und mit unterschiedlichen Algorithmen.

15

Die Funktionen zur Überwachung der Mikrocontroller prüfen neben RAM-, ROM- und Mikroprozessorfunktionen beispielsweise auch, ob die Steuerungs- und Regelungsfunktionen f_n und die Überwachungsfunktionen f_{0n} überhaupt ausgeführt werden. Dies macht den Einsatz eines zweiten Mikrocontrollers im Motorsteuergerät, eines so genannten Überwachungsrechners, notwendig. Die Funktionen zur Überwachung der Mikrocontroller werden auf den Funktionsrechner und den Überwachungsrechner verteilt. Beide überwachen sich in einem Frage-Antwort-Spiel gegenseitig.

20

Als sicherer Zustand ist die Stromabschaltung für die elektromechanische Drosselklappe festgelegt. Die Drosselklappe ist so konstruiert, dass sie nach einer Stromabschaltung selbsttätig die Leerlaufposition einnimmt. Der Übergang in den sicheren Zustand kann deshalb dadurch eingeleitet werden, dass eine Abschaltung der Endstufen des Steuergeräts, die die Drosselklappe ansteuern, erfolgt. Der Motor kann so im Notlauf weiterbetrieben werden.

25

Sowohl die Überwachungsfunktionen f_{0n} , als auch die Funktionen zur Überwachung der Mikrocontroller auf dem Funktions- und auf dem Überwachungsrechner können also die Drosselklappenendstufen des Steuergeräts abschalten.

30

Im Falle eines erkannten Fehlers wird neben dieser Sicherheitsreaktion auch ein Eintrag im Fehlerspeicher vorgenommen. Außerdem wird meist auch eine Information an den Fahrer etwa über eine Anzeige im Kombiinstrument ausgegeben.

5 Soll die Zuverlässigkeit dieses Überwachungskonzepts beurteilt werden, so sind zunächst drei Arten von Funktionen zu unterscheiden:

- die Steuerungs- und Regelungsfunktionen f_n
- die Überwachungsfunktionen f_{0n}
- die Funktionen zur Überwachung der Mikrocontroller

10 Die Zuverlässigkeitsblockdiagramme für diese verschiedenen Funktionen lassen sich dann recht einfach bestimmen (Bild 6):

Bild 6: Zuverlässigkeitsblockdiagramme für Funktionen der Motorsteuerung

15 Um die Systemzuverlässigkeit zu bestimmen, wird man alle drei Arten von Funktionen gleichzeitig fordern. Dann ergibt sich die Systemzuverlässigkeit durch eine Reihenschaltung dieser Blockdiagramme. Zusätzlich müssen auch die Komponenten K_7 und K_8 , die in den Blockdiagrammen der einzelnen Funktionen nicht vorkommen, in Reihe geschaltet werden. Die Systemzuverlässigkeit $R_{S \text{ Zuverlässigkeit}}$ ergibt sich durch Multiplikation der Zuverlässigkeit der drei Funktionen R_X ; $X = A, B, C$ mit der Zuverlässigkeit der Komponenten K_7 R_D und K_8 R_E und ist wegen $R_X < 1$ in jedem Fall geringer als die jeweilige Zuverlässigkeit der Funktionen R_X . Bei
20 der Berechnung der Systemzuverlässigkeit müssen die Regeln für das Rechnen mit mehrfach auftretenden Elementen im Zuverlässigkeitsblockdiagrammen beachtet werden [1].

$$R_{S \text{ Zuverlässigkeit}} = R_A R_B R_C R_D R_E$$

25 Dagegen ist für die Sicherheit lediglich das zuverlässige Erkennen eines Ausfalls und der zuverlässige Übergang in den sicheren Zustand notwendig. Die Zuverlässigkeit $R_{S \text{ Sicherheit}}$ dieser Sicherheitsreaktion wird durch die Zuverlässigkeit der Überwachungsfunktionen f_{0n} oder der Funktionen zur Überwachung der Mikrocontroller vorgegeben und ist deshalb höher als die Zuverlässigkeit der Funktionen R_X . Zudem geht die Zuverlässigkeit der Komponenten K_7 R_D und K_8 R_E in die Berechnung von $R_{S \text{ Sicherheit}}$ nicht ein.
30

$$R_{S \text{ Sicherheit}} = 1 - (1 - R_B)(1 - R_C)$$

5 Wie dieses Beispiel zeigt, können Maßnahmen zur Erhöhung der Sicherheit die Zuverlässigkeit des Systems verringern. Außerdem ist ersichtlich, dass Maßnahmen zur Erhöhung der Zuverlässigkeit zu einer Reduzierung der Sicherheit eines Systems führen können.

10 Obwohl nur Hardware-Komponenten betrachtet werden, haben die Zuverlässigkeits- und Sicherheitsanalysen großen Einfluss auf die Software-Entwicklung. Wie am Beispiel der Bewertung des Überwachungskonzeptes gezeigt, beeinflussen sie etwa die **Zuordnung der Software-Funktionen zu den Mikrocontrollern** in einem verteilten und vernetzten System oder die notwendigen **Qualitätssicherungsmaßnahmen in der Software-Entwicklung**.

Literatur

15 [1] Alessandro Birolini: Zuverlässigkeit von Geräten und Systemen. Springer Verlag, 1997.

Vorgehensweise und Kerngedanken

Schritt 1: Festlegung des Hardware-Netzwerks des elektronischen Systems, d. h. Spezifikation der Mikrocontroller und ihrer Vernetzung.

5 **Schritt 2:** Festlegung der Software-Komponenten, die für die Realisierung der Funktionen des elektronischen Systems erforderlich sind und Spezifikation der Kommunikation zwischen den Software-Komponenten

Schritt 3: Zuordnung der Software-Komponenten zu den Mikrocontrollern des Hardware-Netzwerks

10 **Schritt 4:** Aufstellen der Zuverlässigkeitsblockdiagramme für die geforderten Funktionen des elektronischen Systems ausgehend von den Hardware-Komponenten und Hardware-Verbindungen

Schritt 5: Nachweis der Sicherheit und Zuverlässigkeit durch Berechnung der Zuverlässig-

15 keit für die Sicherheitsfunktionen und der Zuverlässigkeit für die gesamten geforderten Funktionen des elektronischen Systems

Schritt 6: ggf. Wiederholung der Schritte 1 bis 5 und Korrektur der Systemarchitektur, d. h. des Software- und Hardware-Netzwerks, sowie der Zuordnung der Software-Komponenten zu Hardware-Komponenten

20

20.06.2003 Sy

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10

Sicherheits- und Zuverlässigkeitsbetrachtungen für Software-Hardware-Überwachungskonzepte elektronischer Steuergeräte mit Zuverlässigkeitsblockdiagrammen

Zusammenfassung

15

Zuverlässigkeits- und Sicherheitsanalysen umfassen z. B. Ausfallraten- und Ausfallartenanalysen, wie die Ausfallarten- und Wirkungsanalyse (FMEA) oder die Fehlerbaumanalyse (FTA), sowie die Untersuchung und Bewertung von konkreten Möglichkeiten zur Verbesserung der Zuverlässigkeit oder der Sicherheit.

20

Im folgenden wird am Beispiel der formalen Überprüfung von Überwachungskonzepten ein Verfahren zur formalen Überprüfung von Funktionen elektronischer Systeme durch Zuverlässigkeitsblockdiagramme beschrieben. Damit ist die frühzeitige Bewertung unterschiedlicher Überwachungskonzepte elektronischer Steuergeräte im besonderen und von Funktionen elektronischer Systeme im allgemeinen, die durch Software und Hardware realisiert werden, hinsichtlich der erreichbaren Systemsicherheit und der Systemzuverlässigkeit möglich.

25

Die Ergebnisse beeinflussen insbesondere die Verteilung von Software-Funktionen auf die Mikrocontroller vernetzter Steuergeräte und damit die Entwicklung von Software für verteilte und vernetzte Steuergeräte.

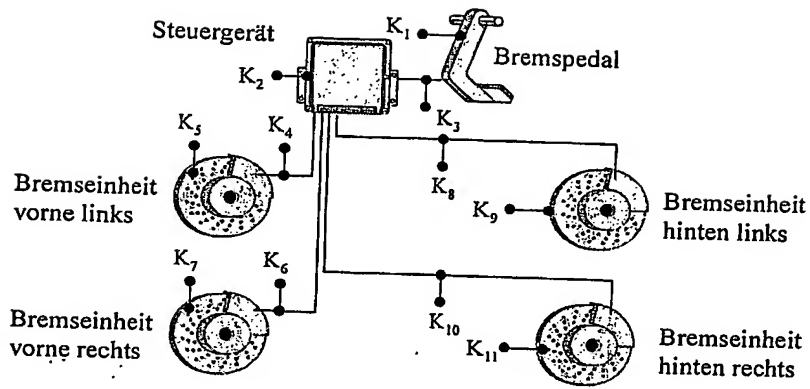


Bild 1: Systemsicht für ein Brake-By-Wire-System

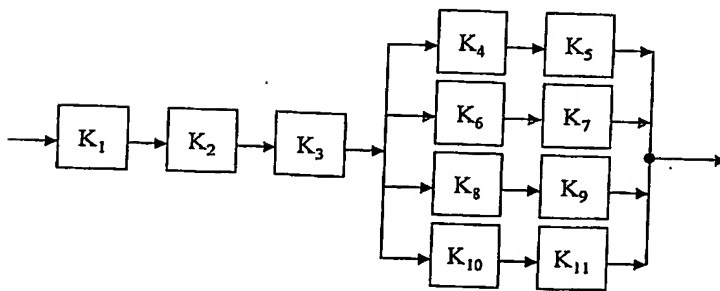


Bild 2: Zuverlässigkeitsblockdiagramm für die Funktion „Bremsen“ des Brake-By-Wire-Systems

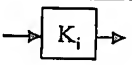
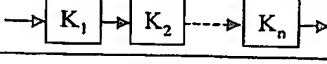
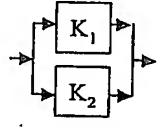
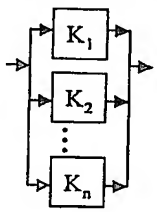
Zuverlässigkeits- blockdiagramm	Zuverlässigkeits- funktion $R_S = R_S(t), R_i = R_i(t)$	Ausfallrate λ_S für $\lambda_i = \text{konstant}$: $R_i(t) = e^{-\lambda_i t}$	Beispiel
	$R_S = R_i$	$\lambda_S = \lambda_i$	
	$R_S = \prod_{i=1}^n R_i$	$\lambda_S = \sum_{i=1}^n \lambda_i$	$R_1 = R_2 = 0,9$ $R_S = 0,9 \cdot 0,9 = 0,81$
 1-aus-2-Redundanz	$R_S = 1 - (1 - R_1)(1 - R_2)$ $= R_1 + R_2 - R_1 \cdot R_2$		$R_1 = R_2 = 0,9$ $R_S = 1 - (1 - 0,9)(1 - 0,9) = 0,99$
 k-aus-n-Redundanz	$R_1 = R_2 = \dots = R_n = R$ $R_S = \sum_{i=k}^n \binom{n}{i} R^i (1-R)^{n-i}$ Für $k = 1$ gilt: $R_S = 1 - (1-R)^n$		$R_1 = R_2 = R_3 = R_4 = 0,9$ bei 1-aus-4-Redundanz: $R_S = 1 - (1 - 0,9)^4 = 0,9999$

Bild 3: Einige Grundregeln zur Berechnung der Zuverlässigkeitsfunktion für das System [1]

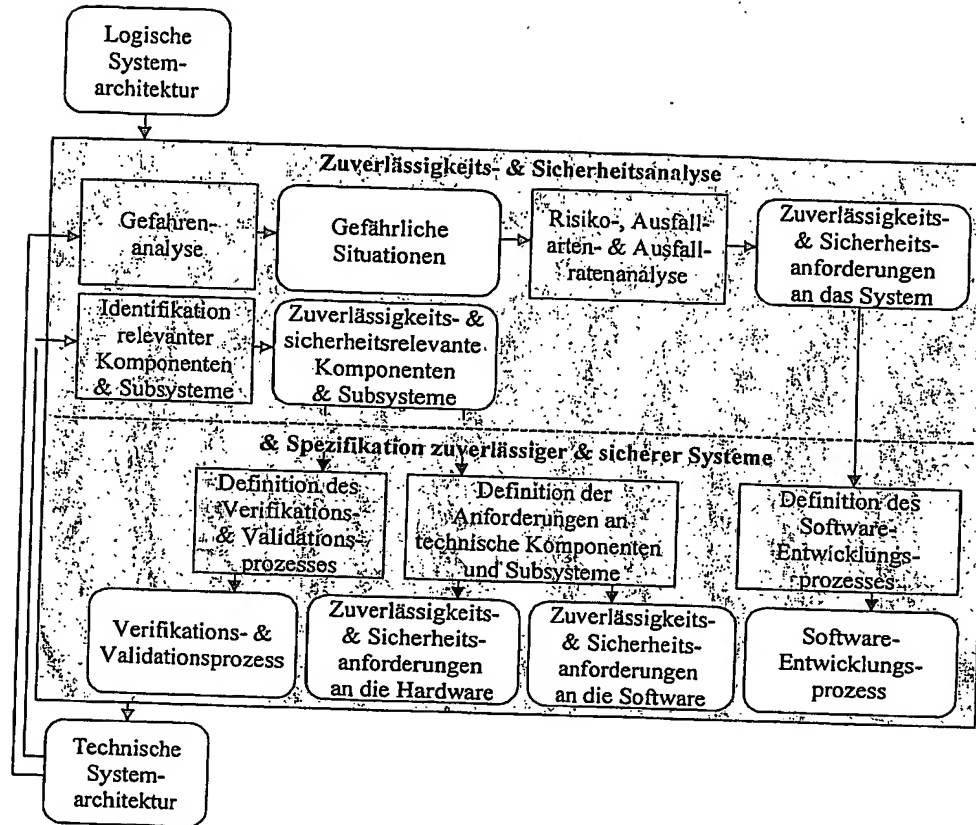


Bild 4: Schritte bei der Zuverlässigkeits- und Sicherheitsanalyse und der Spezifikation zuverlässiger und sicherer Systeme [2]

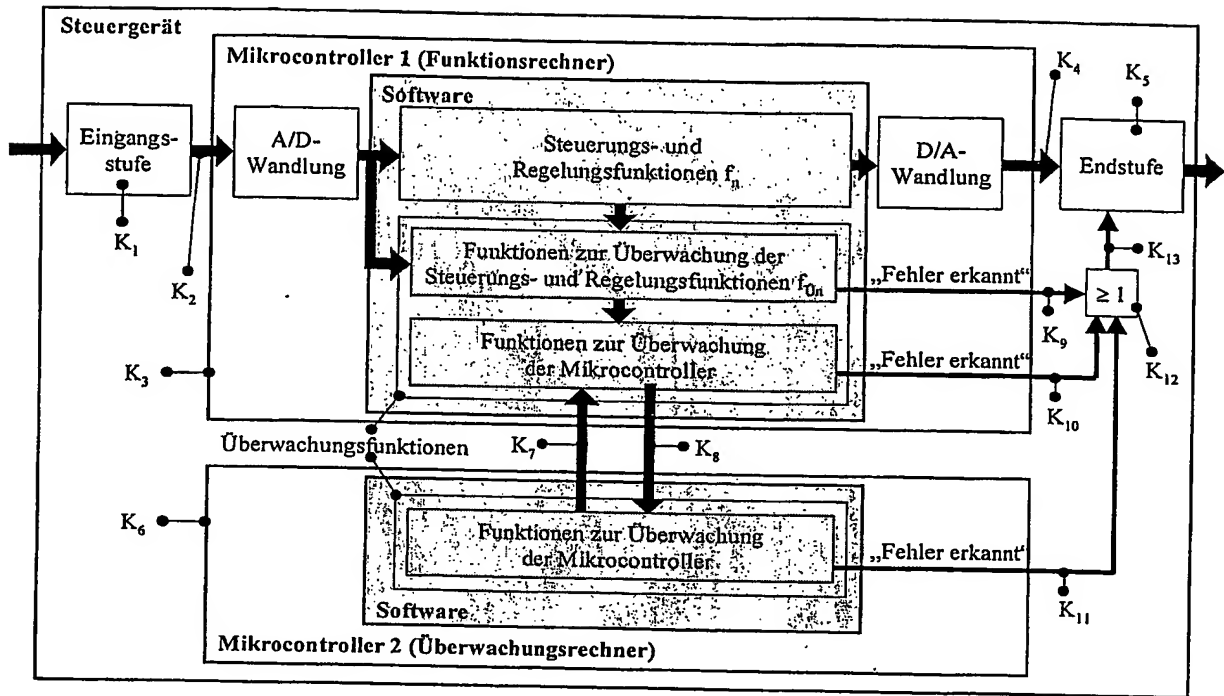


Bild 5: Überwachungskonzept für sicherheitsrelevante Funktionen des Motorsteuergeräts [79]

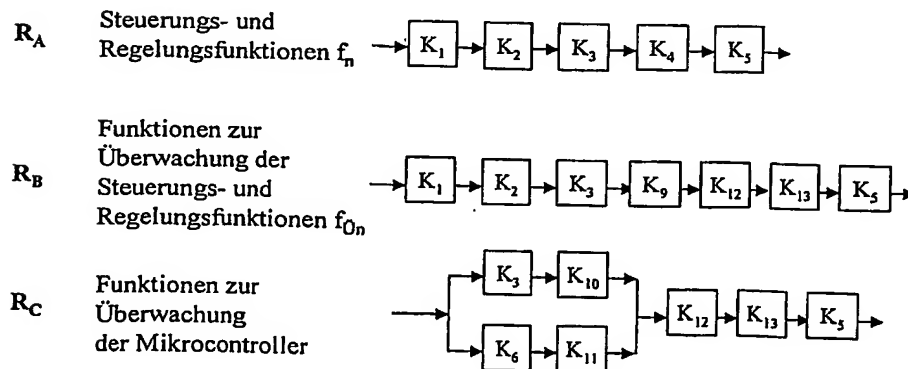


Bild 6: Zuverlässigkeitsblockdiagramme für Funktionen der Motorsteuerung

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.